

ABSTRACT

A method and system are disclosed for securely transmitting a data message. In a method of the invention, a first encrypting key is obtained. A second encrypting key is then generated as a function of the first encrypting key and as a function of an identified parameter. The identified parameter can be time or some other random number. A requirement is that the parties desiring to communicate both have knowledge of the identified parameter. The data message is then encrypted using the second encrypting key to generate an encrypted message. The encrypted message can then be securely transmitted. A party receiving the encrypted message then obtains a first decryption key. A second decrypting key is then generated as a function of the first decrypting key and as a function of the identified parameter. The encrypted message is decrypted using the second encrypting key to recover the data message.